Mobile Device Acceptable Use Policy Template

<Company> grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. <Company> reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of <Company>’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

<Company> employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

The company defines acceptable business use as activities that directly or indirectly support the business of <Company>.

The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the Company. Such websites include, but are not limited to all sites not available on a company computer when operated by the user.

Devices may not be used at any time to:

- Store or transmit illicit materials, including private customer data unless this data is encrypted using company-approved methods.
- Store or transmit proprietary information belonging to another company
- Harass others
- Etc.

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

<Company> has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
Devices and Support

Smartphones approved include all versions of the iPhone running iOS version 4.0 and higher, Android smartphone version 2.2 and higher, all Samsung devices, and Windows Phone 7 and 8. Blackberry phones are not allowed at the current time.

Tablets including iPad running iOS version 4 or above, Android-based tablets running version 3 or above, and Windows 7 or 8 tablets are allowed. Tablets may access email using Outlook Web Access as if a Mobile PC, or through a VPN installed by I.T.

Connectivity issues are supported by I.T. for Wireless Networks installed and approved by the company; employees should contact the device manufacturer or their carrier for operating system or hardware-related or cellphone data network issues.

Devices must be presented to I.T. for proper installation and configuration of security software before they can access the network.

Reimbursement

The company will not reimburse the employee for the cost of the device unless agreed upon in the employee’s contract.

The company will not a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc. unless agreed upon in the employee’s contract.

The company will not reimburse the employee for the following charges: roaming, plan overages, etc. unless agreed upon in the employee’s contract.

Security

In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network. Device passwords must be a minimum of 4 characters.

- The device must lock itself with a password or PIN if it’s idle for five minutes.
- After five failed login attempts, the device will lock. Contact I.T. to regain access.
Rooted (Android) or Jailbroken (iOS) devices are strictly forbidden from accessing the network.

Employees are not automatically prevented from downloading, installing and using any app that does not appear on the company’s list of approved apps, but may be asked to remove apps that have the potential for creating a risk for which the company would become liable.

Smartphones and tablets that are not on the company’s list of supported devices are not allowed to connect to the network.

Employees’ access to company data is limited based on user profiles defined by I.T. and automatically enforced.

The employee’s device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) I.T. detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

**Risks/Liabilities/Disclaimers**

While I.T. will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.

The company reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company’s acceptable use policy as outlined above.

The employee is personally liable for all costs associated with his or her device.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

<Company> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

I have read and agree to the terms of this Mobile Device Acceptable Use Policy.

Print Name, Sign and Date ________________________________